Руководство по выполнению нормативных требований в бизнесе

Планируйте обработку электронных данных сегодня, & чтобы избежать юридических рисков завтра

Синтия Л. Джексон

Baker & McKenzie





Синтия Л. Джексон

Партнер, Baker & McKenzie LLP

Синтия Л. Джексон является партнером в расположенном в Пало-Альто, штат Калифорния, офисе компании Baker & McKenzie – крупнейшей юридической фирмы в мире, представительства которой расположены в 38 странах. Она является автором буклета "Руководство по выполнению нормативных требований в бизнесе", предназначенного для руководителей высшего звена, в котором представлена информация о широком спектре проблем, связанных с соблюдением требований нормативных документов, правительственных предписаний и требований по использованию технологии e-Discovery. Синтия Джексон благодарит Джона Раудабог, партнера компании в офисе в Чикаго, за предоставленные материалы относительно контроля вопросов трудоустройства, опубликованные в рамках экспертного заключения по спору компании *The Guard Publishing Company и профессионального объединения Eugene Newspaper Guild,* который был подан в NLRB 9 февраля 2007 года.

Адвокат Синтия Джексон представляет компании в судебных процессах и дает консультации по вопросам американских и международных законов о трудоустройстве, включая иски о дискриминации и сексуальных домогательствах, разработки и реализации кадровой политики, заключения и расторжения трудовых соглашений, сокращения кадров, кодексов поведения, обеспечения конфиденциальности, социальной ответственности компании, защите конфиденциальной информации и коммерческой тайны, а также по вопросам последствий слияния и поглощения для сотрудников компаний.

Синтия Джексон была признана одним из "Лучших юристов США" и неоднократно получала титул "Суперюрист Северной Калифорнии". Она закончила Стэнфордский университет и юридический факультет университета штата Техас (оба – с отличием).

Синтия Л. Джексон, адвокат
Baker & McKenzie LLP
660 Hansen Way, Palo Alto, California 94304, USA
Телефон: +1 650-856-5572 Факс: +1 650-856-9299
cynthia.l.jackson@bakernet.com





Содержание





Актуальность проблемы?

В современном мире, где электронные данные играют все большую роль, компаниям необходимо искать такие способы обработки данных, которые позволят эффективно контролировать риски, связанные с соблюдением требований нормативных документов. Увеличение объема электронных данных удивляет и ошеломляет. Запоминающие устройства современных компьютеров обладают такой емкостью, что даже самая скромная небольшая компания располагает хранилищем электронных данных, объем которого соответствует 2000 шкафов с четырьмя ящиками для папок.[1] Задача управления электронными данными осложняется тем фактом, что теперь данные представляют собой не материальные листы бумаги, а байты информации, которые постоянно редактируются, изменяются и обновляются разными людьми и из различных источников. Использование в компании надлежащих средств архивирования, хранения, мониторинга, фильтрации и шифрования электронных данных уже не является проявлением доброй воли компаний: теперь использование таких средств регламентируется нормативными документами.

Использование в компании надлежащих средств архивирования, хранения, мониторинга, фильтрации и шифрования электронных данных уже не является проявлением доброй воли компаний: теперь использование таких средств регламентируется нормативными документами.

Современные информационные системы используются для управления промышленным оборудованием, обработки финансовых данных, контроля складских запасов, размещения заказов, а также передачи изображений и документов. Внедрение таких систем позволило существенно повысить скорость вербальных и невербальных коммуникаций. Электронная почта является одним из наиболее распространенных

[1] Jason Krause, *E-Discovery Gets Real,* ABA JOURNAL, February 2007; также см. George L. Paul & Bruce H. Nearon, *The Discovery Revolution: A Guide to the E-Discovery Amendments to the Federal Rules of Civil Procedure,* ABA SECTION OF SCI & TECH. LAW.

способов передачи информации, но электронные коммуникации не ограничиваются только электронной почтой; вспомните об интернет-дневниках (которые часто называют блогами), программах для мгновенного обмена сообщениями (которые обеспечивают общение пользователей в режиме реального времени), веб-камерах для видеоконференций, средствах передачи документов и видеоматериалов, а также о средствах передачи голоса по широкополосной сети. Однако такие системы могут стать объектом ненадлежащего использования, что может нанести вред бизнес-деятельности. Люди могут отправлять сообщения сексуального характера или сообщения с угрозами сотрудникам, менеджерам, а также сторонним лицам; пользователи могут загружать (на самом деле, красть) объекты интеллектуальной собственности из систем компаний или сторонних лиц, порочить компанию, ее продукцию и услуги, заказчиков и конкурентов; наконец, пользователи могут скрытно передавать украденную информацию в удаленные системы или хранить такую информацию на запоминающих устройствах, предоставленных компанией. Пользователи могут демонстрировать или распространять материалы, которые суд может признать материалами, связанными с сексуальными домогательствами или не соответствующими законодательству, создавать и размещать дискредитирующие материалы в Интернете на сайтах и в блогах, а также организовывать или даже совершать преступления. Все эти действия могут выполняться нарабочем месте с негласным использованием оборудования, предоставленного компанией.[2]

[2] *Electronic Workplace: Is Your Company's Work Blogging Down?* FEDERAL EMPLOYMENT LAW INSIDER, September 2006; Michael R. Phillips, *Inappropriate Use of Email by Employees and System Configuration Management Weaknesses Are Creating Security Risks,* Treasury Inspector General for Tax Administration, July 31, 2006.

Неудивительно, что 86% главных юридических советников, которые участвовали в исследовании, проведенном ассоциацией юридических советников корпораций (ACC), указали в качестве основной проблемы "отслеживание операций компании, которые могут повлечь за собой юридические последствия".[3] До 2005 года 24% компаний получали судебные повестки, связанные с использованием электронной почты, и 15% компаний участвовали в судебных процессах, причиной которых послужило использование электронной почты сотрудниками компании. По данным того же исследования, 10% сообщений электронной почты в системах компаний являлись сообщениями сексуального, романтического или порнографического характера.[4] Даже до 1 декабря 2006 года, когда в силу вступили правила использования технологии e-Discovery, регламентируемые федеральными правилами гражданского судопроизводства (FRCP), в 2004 году более 20% компаний получали повестки в суд в связи с использованием электронных коммуникаций, о котором стало известно в ходе судебного процесса или правительственного расследования.[5] Значение этого показателя более чем вдвое превышает значение аналогичного показателя за 2001 год.[6] Фактически, в 2005 году американские компании потратили 1,2 млрд долларов США на услуги внешних компаний по реализации технологии e-Discovery.[7] Ожидается, что в 2006 году эта сумма составит 1,9 млрд долларов США.[8] С принятием правил использования технологии e-Disco-ery в соответствии с FRCP, можно предполагать существенное увеличение этой суммы в ближайшее время. Вместе с тем результаты исследования,

До 2005 г. 24% компаний получали повестки в суд и 15% компаний участвовали в судебных процессах, причиной которых послужило использование электронной почты сотрудниками компании.

В 2005 году американские компании потратили 1,2 млрд долларов США на услуги внешних компаний по реализации технологии e-Discovery. Ожидается, что в 2006 году эта сумма составит 1,9 млрд долларов США.

[3] ACC & SERENGETI, MANAGING OUTSIDE COUNSEL SURVEY REPORT, October 23, 2006.
[4] *2006 Workplace E-mail, Instant Messaging & Blog Survdey: Bosses Battle Risk by Firing E-mail, IM & Blog Violators,* AMA, July 11, 2006, http://www.amanet.org/press/amanews/2006/blogs_2006.htm.
[5] AMA/ePolicyInstitute Research, *2004 Workplace E-mail and Instant Messaging Survey Summary,*at 1.
[6] *Id.*
[7] Sacha Consulting, Ramon Nunez, Metal INCS, Gregory McCurdy, Microsoft Corp, ABA Digital Evidence Project, The National Law Journal/ www. NLJ.com, September 19, 2005.
[8] *Id.*

проведенного всего за два месяца до вступления поправок FRCP в силу, оказались неожиданными: только 7% юридических советников корпораций сообщили, что их компании готовы к вступлению в силу поправок к правилам, а 54% даже не знали, что поправки вступят в силу в декабре 2006 года.[9]

Кроме того, компании должны выполнять требования растущего количества нормативных документов, регламентирующих электронные коммуникации в условиях постоянного появления новых инициатив.[10] Множество документов регламентируют защиту конфиденциальных личных данных, *например:* Федеральный закон о конфиденциальности электронных коммуникаций, принятый в 1986 году[11]; Закон о преемственности страхования и отчетности в области здравоохранения, принятый в 1996 году[12]; Закон о защите личных данных детей в Интернете, принятый в 1998 году[13]; Акт Грэмма-Лича-Блайли, принятый в 1999 году[14]; Закон об ограничении рассылки незапрошенных порнографических и маркетинговых материалов, принятый в 2003 году[15]; Закон штата Калифорния об уведомлениях о нарушениях безопасности, принятый в 2002 году[16]; Закон штата Калифорния о защите персональных данных, принятый в 2004 году[17] и многие другие законы и нормативные документы США и других стран.[18]

Компании должны не только соблюдать законы, регламентирующие уничтожение и хранение документов, но и постоянно совершенствовать

[9] Lexis Nexis® Applied Discovery® survey completed at the ACC 2006 Annual Meeting in October 2006.
[10] *Data Security: Federal and State Laws,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, February 3, 2006; *Data Security: Federal Legislative Approaches,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, February 9, 2006; *Obscenity and Indecency: Constitutional Principles and Federal Statutes,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, June 25, 2003.
[11] 18 U.S.C. § 101 *и последующие.*
[12] 42 U.S.C. § 201 *и последующие.*
[13] 15 U.S.C. § 6501 *и последующие.*
[14] 15 U.S.C. §§ 6801-6809.
[15] 15 U.S.C. §§ 7701-7713.
[16] Cal. S.B. 1386 (2002) (Cal. Civ. Code §§ 1798.82 и фрагменты 1798.29).
[17] Cal. Civ. Code § 1798.81.5 (Cal. A.B. 1950 (2004)).
[18] Allan Holmes, *The Global State of Information Security 2006,* CIO MAGAZINE, September 15, 2006.

средства защиты от злоумышленников и предотвращать возможность хищения интеллектуальной собственности с использованием систем электронной обработки данных.[19] Интернет может стать средством доступа посторонних лиц к самым ценным ресурсам компании. В 2004 году доля незапрошенных сообщений электронной почты составляла 73% от всех входящих сообщений; в 2006 году значение этого показателя увеличилось до 93%.[20] Большинство таких сообщений вызывают досаду или служат причиной напрасной траты времени, однако вредоносные вложения, например вирусы, интернет-черви, модули загрузки, троянские программы, модули рассылки спама, спам с использованием ссылок, фишинговые атаки и вложения для атак фарминга могут представлять собой угрозу для работы корпоративной сети, а также хранящейся в ней бизнес-информации и интеллектуальной собственности.[21] Посторонние лица могут "взломать" корпоративные системы, получить доступ к коммерческой тайне и конфиденциальной информации, украсть пароли или установить перенаправление пользователей на сайты, которые выполняют несанкционированную загрузку вредоносного программного обеспечения на компьютер пользователя. Считается, что 33% таких атак проводятся пользователями внутренней сети.[22]

Доля незапрошенных сообщений электронной почты составляет 93% от всех входящих сообщений электронной почты.

Сорок процентов респондентов, участвовавших в недавнем исследовании Национального центра США по применению суперкомпьютеров (NCSA), сообщили,

[19] *Интернет: An Overview of Key Technology Policy Issues Affecting Its Use and Growth,* CRS REPORT FOR CONGRESS, April 13, 2005.
[20] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004); W*ireless Privacy and Spam: Issues for Congress,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, December 22, 2004; *'Junk E-mail': An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam"),* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, April 15, 2003; *Cybercrooks Deliver Trouble,* WASHINGTON POST, December 27, 2006, D1.
[21] *Pharming,* WEBSENSE, INC. (2006); *The Economic Impact of Cyber-Attacks,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS, April 1, 2004.
[22] Scott Berinato, *The Global State of Information Security 2005,* PRICE WATERHOUSECOOPERS AND CIO, September 15, 2005

что они посещают сайты социальных сетей с рабочих компьютеров, тем самым подвергая корпоративную сеть опасности вторжения злоумышленников.[23] (68% опрошенных компаний сообщили, что в 2004 они подвергались атакам; 43% этих компаний сообщили о факте несанкционированного доступа к информации, системам или сетям, при этом 14% сообщили о краже интеллектуальной собственности).[24] В действительности, из недавно опубликованных судебных документов стало известно, что старший исследователь компании DuPont загрузил в течение менее чем пяти месяцев 22000 конфиденциальных документов и перенес 180 документов компании DuPont на свой ноутбук, а затем предоставил эти документы своему новому работодателю. В документах содержалась информация об "основных технологиях и линейках продуктов компании DuPont, а также сведения о новых и перспективных технологиях, находящихся на стадии исследования и разработки. "Стоимость документов была оценена в 400 млн долларов США.[25]

Юридически корректные или "безвредные" действия сотрудников также могут привести к повышению расходов компании, при этом искушение совершать такие "безвредные" действия трудно переоценить. По результатам исследования, проведенного в 2004 году в 840 компаниях США, 66% респондентов сообщили, что время ежедневного использования сотрудниками систем компании в личных целях не превышает 2 часов, 24% респондентов оценили это время в 2-3 часа и 10% респондентов сообщили, что системы компании ежедневно используются сотрудниками компании в личных целях более 4 часов.[26] В ходе того же исследования было установлено,

[23] *CA/NCSA Social Networking Study Report,* RUSSELLRESEARCH.COM, at 4, http://staysafeonline.org/features/SocialNetworkingReport.ppt.
[24] *2005 E-Crime Watch Surve y- Survey Results,* CSO MAGAZINE, U.S. SECRET SERVICE, CERT COORDINATION CENTER., http://www.csoonline.com/info/ecrimesurvey05.pdf.
[25] David Kauffman, *How Safe Is Your Data?,* HR HERO LINE, March 9, 2007.
[26] AMA/ePolicy Institute Research, *2004 Workplace E-mail and Instant Messaging Survey* (2004).

что 75% сотрудников ежедневно отправляют или получают не более 10 личных сообщений электронной почты.[27] Девяносто процентов сотрудников ежедневно тратят до 90 минут на личное общение с помощью программ для мгновенного обмена сообщениями, 19% этих сотрудников добавляют вложения в текстовые сообщения, 16% распространяют шутки, слухи или пренебрежительные отзывы, 9% сотрудников разглашают конфиденциальную информацию и 6% сотрудников отправляют сообщения сексуального, романтического или порнографического характера.[28]

Сочетание юридических требований, обязательных к выполнению, и технических рекомендаций, реализуемых компаниями по собственной воле, вынуждает компании проводить планирование и реализацию надлежащих мер, а также обучение сотрудников *до того,* как компании столкнутся с юридическими последствиями действий своих сотрудников. Только немногие компании могут позволить себе роскошь неторопливо обдумывать эти проблемы и начать действовать только тогда, когда подан первый юридический иск, состоялось хищение интеллектуальной собственности, произошло раскрытие конфиденциальных данных или сформировалась неблагоприятная рабочая среда. Большинству компаний необходимо планировать свои действия заранее. Во-первых, компаниям необходимо разработать систему сохранения, архивирования и мониторинга процесса передачи данных. Во-вторых, необходимо реализовать систему шифрования конфиденциальной информации и внедрить систему контроля и разграничения доступа. В третьих, компаниям необходимо проводить постоянное обучение сотрудников и аудит выполнения установленных процессов и политик.

[27] *Id.*
[28] *Id.*





Кого это волнует или должно волновать?

Вопросы управления электронными данными затрагивают практически всех сотрудников компании: главного юридического советника и его помощников, лиц, ответственных за выполнение нормативных требований, внутренних аудиторов, сотрудников финансового подразделения, руководителей ИТ-подразделения, персонал отдела кадров и мотивации сотрудников, сотрудников отдела лицензирования и защиты интеллектуальной собственности, руководителей цепочки поставок, сотрудников отдела экспортного контроля, сотрудников отдела продаж и бизнес-персонал.

Например, компании США, акции которых представлены на бирже, должны выполнять требования по формированию отчетности, аудиту и прозрачности действий, установленные Актом Сарбейнса-Оксли (SOX), а также требования по хранению записей и ведению учета, установленные Актом о коррупционных действиях при работе за пределами США. Кроме того, компании, против которых подан иск в федеральный суд или для которых существует угроза подачи такого иска, должны обладать средствами для сохранения соответствующих электронных данных. Компании, работающие в банковской и финансовой сферах, а также в сфере здравоохранения, должны выполнять подробные юридические и нормативные требования, связанные с использованием, доступом и распространением информации. Те компании,

Компании, против которых подан иск в федеральный суд или для которых существует угроза подачи такого иска, должны обладать средствами для сохранения соответствующих электронных данных.

От этого не застрахована ни одна компания. Кроме того, малым и средним компаниям следует заранее планировать внедрение таких систем.

которые работают на международном рынке или экспортируют оборудование или программы, обязаны управлять своими данными, включая процедуры их шифрования, в соответствии со сложными и порой противоречивыми процедурами.

Но век электронных данных ставит новые задачи даже перед теми компаниями, акции которых не представлены на бирже, которым не угрожает юридическое разбирательство, которые не работают в сферах индустрии с особым регулированием, а также не занимаются внешнеэкономической деятельностью. Исследования показали, что примерно тридцать процентов краж данных совершаются сотрудниками компаний, и что огромное количество дающих основание для судебного преследования унизительных и дискриминационных действий, а также сексуальных домогательств *совершаются* авторизованными пользователями.[29] От этого не застрахована ни одна компания. Кроме того, малым и средним компаниям следует заранее планировать внедрение систем, позволяющих защитить интеллектуальную собственность, защитить их сотрудников от обвинений в создании неблагоприятной рабочей среды или предотвращать удаление документов, которые могут потребоваться в случае юридического разбирательства.

По иронии судьбы, именно те технологии, которые вызвали появление множества задач, связанных с увеличением объема данных, могут оказаться полезными при создании решения,

[29] Scott Berinato, *The Global State of Information Security 2005,* PRICE WATERHOUSECOOPERS AND CIO, September 15, 2005.

обеспечивающего хорошо спланированный и управляемый электронный документооборот, который полностью соответствует юридическим и нормативным требованиям. В состав таких электронных систем должны входить программные комплексы, обеспечивающие возможность сохранения и архивирования документов, защиты от удаления документов, контроля доступа с использованием шифрования (если это требуется), а также мониторинга и ограничения доступа в Интернет, если эти действия разрешены принятыми в организации политиками и действующим законодательством. Необходимо не только установить такие системы, но и обязательно проанализировать соответствующие юридические требования, а также обучить сотрудников работе с системами управления электронными данными, чтобы установить такие правила обработки бизнес-информации, которые позволят быстро собрать необходимые электронные данные при появлении юридической необходимости. Выбор и развертывание систем управления электронными данными, создание и обеспечение выполнения политик, а также постоянное обучение пользователей и аудит работоспособности системы *до возникновения юридической необходимости* требуют скоординированной и вдумчивой совместной работы сотрудников всех подразделений, включая главного юридического консультанта, отдел кадров и т. д.

Выбор и развертывание систем управления электронными данными, создание и обеспечение выполнения политик, а также постоянное обучение пользователей и аудит работоспособности системы *до возникновения юридической необходимости* требуют скоординированной и вдумчивой совместной работы сотрудников всех подразделений.





Законодательные требования к ведению электронных записей

Незнание новых поправок к федеральным правилам гражданского судопроизводства может привести к колоссальным расходам.

При отсутствии "ситуации юридического разбирательства" компании, как правило, не обязаны обеспечивать сохранение электронных данных (или других записей), хотя сохранение записей определенного типа, например, налоговой отчетности, сведений о трудоустройстве и корпоративной документации может регламентироваться различными федеральными законами или законами штата. Возникновение "ситуации юридического разбирательства" вынуждает обеспечить сохранение соответствующей информации, при этом от компании требуется пересмотреть существующую практику уничтожения документов. Новые дополнения FRCP регламентируют необходимость "хранения документов в связи с юридическим разбирательством". Такой подход распространяется на документы, которые по мнению компании могут потребоваться при проведении юридического разбирательства. Режим "хранения документов в связи с юридическим разбирательством" может инициироваться задолго до начала непосредственного юридического разбирательства, например в случае, когда компания получает внутреннюю жалобу "представителю руководства" "уведомление о необходимости сохранения документов от потенциального участника юридического разбирательства или его адвоката, документы об открытии судопроизводства,

Суд обязал компанию оплатить судебные издержки и расходы на адвоката истца, поскольку компания не обеспечила сохранение необходимых сообщений электронной почты и данных, а также гарантировать сохранение необходимой информации с *момента поступления внутренней жалобы от сотрудника* о сексуальных домогательствах.

уведомление о расследовании, проводимом государственными органами, судебную повестку или запрос государственных органов о передаче информации, а также в случае, когда против компании выдвигаются административные обвинения. При возникновении "ситуации юридического разбирательства" в соответствии с новыми поправками компания должна принять меры для прекращения удаления всех документов и обеспечения сохранения всех записей, включая электронные данные, а также возможно содержащиеся в них метаданные, которые, как известно или должно быть известно компании, могут потребоваться для проведения юридического разбирательства или при разумных допущениях могут помочь в обнаружении доказательств.

Даже до принятия недавних поправок к FRCP суды негативно относились к компаниям, которые не обеспечили сохранение данных, о которых было или могло быть известно, что они могут потребоваться в ходе судебного разбирательства. В деле *Broccoli против Echostar Communications Corp,* 229 F.R.D. 506 (D.C. Md. 2005), суд принял решение, что работодатель обязан обеспечить сохранение электронных документов в течение 11 месяцев, предшествующих увольнению сотрудника (и истца по этому делу). Возникновение такой обязанности вызвано тем, что истец уведомлял своего работодателя, как устно, так и по электронной почте, о сексуальных домогательствах на работе. Суд обязал компанию оплатить судебные издержки и расходы на адвоката истца, поскольку компания не

смогла прекратить удаление сообщений электронной почты и данных и гарантировать сохранение необходимой информации с *момента поступления внутренней жалобы от сотрудника* о сексуальных домогательствах.

В серии исков, включающих иски по делам *Zubulake против UBS Warburg LLS,* 220 FRD 212 (S.D. N.Y. 2004), 229 F.R.D. 422 (S.D. N.Y. July 20, 2004 Zubulake II) и 231 FRD 159 (S.D.N.Y. February, 3, 2005 Zubulake III), суд постановил, что компания обязана обеспечивать сохранность электронных документов за 4 последних месяца до дня подачи жалобы о дискриминации (и за 10 месяцев до подачи иска в федеральный суд), поскольку компания знала или должна была знать о том, что соблюдение политики уничтожения документов может привести к уничтожению тех документов, которые могут потребоваться суду. При рассмотрении дела *Zubulake* суд обнаружил, что резервные копии данных ответчика были вероятным источником соответствующих доказательств, но сотрудники, не принадлежащие к юридическому отделу, самовольно удалили соответствующие документы, что потребовало от ответчика выполнить дорогостоящую процедуру восстановления данных.

В деле *Wiginton против CB Richard Ellis,* 229 F.R.D. 568 (N.D. Ill. 2003), суд решил, что компания была уведомлена о необходимости предпринять соответствующие действия письмом советника истца, в котором были указаны документы и упомянуты лица, совершавшие сексуальные домогательства, через несколько дней после подачи иска в суд. В частности

суд постановил, что компания обязана сохранять информацию на жестких дисках компьютеров, почтовые аккаунты и записи журналов действий в Интернете лиц, которые обвиняются в сексуальных домогательствах, или лиц, причастных к этому обвинению. Кроме того, суд рекомендовал истцу подать прошение о возобновлении дела о привлечении ответчика к ответственности за неспособность предоставить электронные данные, связанные с истцом и десятью лицами, обвиняемыми в сексуальных домогательствах, если необходимые удаленные электронные документы будут обнаружены на носителях с резервными данными компании. В деле *Consolidated Aluminum Corp против Alcoa, Inc.,* 2006 U.S. Dist. LEXIS 66642 at *18 (M.D.La. 2006), суд обязал компанию Alcoa оплатить сбор показаний всех ключевых участников процесса, а также затраты и расходы на рассмотрение заявления и изучение недостатков доказательств, поскольку компания Alcoa, отправив собственное требование в компанию Consolidated Aluminum, не прекращала следовать своей внутренней политике удаления документов в течение двух с половиной лет. В деле *Samsung Elecs. Co. против Rambus, Inc.,* 2006 U.S. Dist. LEXIS 50007 (E.D.Va. 2006), ответчик и истец по встречному иску компания Rambus планировала подать иск, указав наиболее вероятную цель иска, возможные юридические претензии и соответствующие документы для сохранения и уничтожения до того, как в самой компании было выполнено фактическое уничтожение информации. Сделав выводы, что компания Rambus преднамеренно уничтожила важные данные, суд указал, что он может обязать компанию Rambus предоставить необходимую

информацию. В свою очередь компания Rambus отозвала встречный иск до того, как суд наложил на нее обязательства по предоставлению информации.

Последствия выполнения обычной политики уничтожения документов и невыполнения требований по хранению документов в связи с юридическим разбирательством могут оказаться ужасающими. В деле *Zubulake* суд не только обязал ответчика оплатить расходы на сбор информации, но, что гораздо важнее, суд предоставил присяжным "рекомендацию по выводам в пользу противоположной стороны". Так, суд постановил, что присяжные могут сделать вывод, что уничтоженные документы могли бы помочь истцам в обосновании их иска о дискриминации, поскольку ответчик не обеспечил хранение документов с даты подачи жалобы в комиссию по вопросам равных возможностей занятости, которая подается за 10 месяцев до любого судебного иска. Присяжные вынесли вердикт, что ответчик должен выплатить 29 млн долларов США. В деле *United States против Philip Morris USA Inc.,* 327 F. Supp. 2d 21 (D.D.C. 2004), суд обязал компанию Phillip Morris выплатить 2,75 млн долларов США, рассчитанные как 250 000 долларов США штрафа за каждого из 11 менеджеров, которые не следовали политике компании по сохранению электронных записей. Кроме того, суд отказался выслушивать объяснения всех одиннадцати менеджеров, которые не соблюдали политику компании по сохранению данных, в ходе судебного разбирательства. В деле *Krumwiede против Brighton Associates LLC,* 2006 U.S. Dist. LEXIS 31669 (N.D. Ill. 2006), суд принял несостязательное решение, поскольку истец (и ответчик по встречному

В дополнение к финансовым санкциям суды также могут привлекать участников процесса к административной или уголовной ответственности за уничтожение доказательств.

FRCP обязывает стороны, участвующие в процессе, вести открытые дискуссии и сотрудничать друг с другом по всем вопросам, связанным с обработкой электронных данных, с самого начала процесса и в ходе судебного разбирательства.

иску) не обеспечил режим хранения документов в связи с судебным разбирательством перед передачей ноутбука эксперту суда, а продолжал работать с файлами на компьютере (удалял, изменял, модифицировал и осуществлял доступ к файлам). Суд счел, что такие действия могли привести к изменению метаданных, хотя и не к полному их удалению. В деле *Dempsey против Pfizer,* 813 S.W. 2d 205 (1991), суд штата Техас отклонил иск в размере 42 млн долларов США в качестве санкции за удаление документов.[30]

В дополнение к представленным выше примерам денежных штрафов и рекомендаций о выводах в пользу противной стороны суды также могут привлечь участников процесса к административной или уголовной ответственности за уничтожение доказательств. Фрэнку Каттроне, бывшему руководителю отдела инвестиций в высокие технологии в банке Credit Suisse First Boston, пожизненно запрещено работать в финансовой сфере, кроме того он был обязан уплатить штраф в 30000 долларов США национальной ассоциации фондовых дилеров. Ранее Фрэнк обвинялся в создании помех правосудию и был приговорен к18 месяцам тюремного заключения за сообщение электронной почты, которое он отправил коллегам по отделу в ходе расследования, проводившегося комиссией по ценным бумагам. В этом сообщении содержалась инструкция "вычистить файлы".

Вышеуказанные примеры наглядно демонстрируют, что поправки к FRCP позволили формализовать те

[30] Эти процессы, прошедшие до принятия поправок к FRCP, не были из ряда вон выходящими. В деле *"В деле Re Quintus Corp. против Avaya, Inc.",* 2006 Bank.LEXIS 2912 (Bank. D. De. 2006), суд принял решение о выплате суммы в 1,88 млн долларов США на основании преднамеренного и признанного наносящим вред уничтожения доказательств, которые ответчик должен был хранить в соответствии с нормативными требованиями и в ожидании юридического разбирательства. В деле *3M Innovation Properties C. против Tomar Electronics, Inc.,* 2006 U.S. Dist. LEXIS 80571 (D. Minn 2006), суд дал рекомендацию о выводах в пользу противной стороны, поскольку ответчик не обеспечил сохранение данных в связи с юридическим разбирательством. В деле Re Napster, 462 F.Supp.2d 1060, 107 -78 (N.D. Cal. 2006), неспособность ответчика своевременно обеспечить сохранение данных в связи с юридическим разбирательством вынудила суд дать рекомендацию о выводах в пользу противной стороны. *Re NTL, Inc. Sec. Litig., 2007* U.S. Dist LEXIS 9110 (S.D.N.Y. 2007), суд установил, что заново сформированная после банкротства корпорация не обеспечила сохранение документов, что повлекло за собой рекомендацию о принятии решения в пользу противной стороны и финансовые санкции. В декабре 2006 года национальная ассоциация фондовых дилеров (NASD) заявила, что компания Morgan Stanley сделала ложное заявление о том, что миллионы сообщений электронной почты были утрачены в ходе террористической атаки на Всемирный торговый центр 11 сентября 2001 года. Это дело еще не завершено.

подходы, которые федеральные суды[31] и некоторые суды штатов применяли в течение нескольких лет. Однако принятие поправок к FRCP также влияет на обязанности участников юридического разбирательства, по крайней мере, в двух аспектах: 1) в поправках явно оговаривается использование технологии e-Discovery, а также обязанности сторон, участвующих в разбирательстве, и их адвокатов по изучению, сохранению, формированию и взаимодействию касательно электронных данных, не оставляя дискуссий по поводу того, требуются ли при рассмотрении иска электронные данные и 2) поправки обязывают стороны, участвующие в разбирательстве, вести открытые дискуссии и сотрудничать друг с другом по вопросам, связанным с обработкой электронных данных с самого начала процесса и в ходе судебного разбирательства. От сторон, участвующих в разбирательстве, требуется в течение первых месяцев разбирательства "встретиться и достичь согласия" по общим вопросам, связанным с обеспечением хранения информации, формата, в котором будет представлена электронная информация (*например* PDF, TIFF, в исходном формате, распечатанной на бумаге и т. п.), считает ли какая-либо из сторон какие-либо данные "недоступными", а также способы разрешения вопросов, связанных с "неоправданно дорогостоящими или трудоемкими" процедурами извлечения данных, а также раскрытием по неосторожности информации, связанной с общением адвоката и клиента, отнесенной к коммерческой тайне, конфиденциальной информации или информации, не подлежащей оглашению, которая

[31] В августе 2006 года юридическая конференция судей штатов утвердила *"Принципы, принятые судами штатов при рассмотрении исков касательно представления информации, хранящейся в электронном виде"*. Тем не менее, эти принципы не являются обязательными до тех пор, пока они не будут утверждены соответствующим штатом. На момент написания книги вопрос утверждения Принципов рассматривался в Массачусетсе и Северной Каролине. Напротив, 1 сентября 2006 года в штате Нью-Джерси были утверждены правила представления информации по технологии e-Discovery, соответствующие модели FRCP. В штатах Аризона, Флорида, Айдахо, Мэриленд и Нью-Гемпшир также рассматривают правила, сходные с поправками в FRCP. Тот факт, что в различных штатах принимаются схожие, но имеющие небольшие различия правила предоставления информации по технологии e-Discovery, подчеркивают необходимость создания таких систем управления электронными данными, которые будут соответствовать общепринятым правилам внедрения технологии e-Discovery и допускать небольшие отклонения в соответствии с нюансами законодательства определенного штата.

может попасть в формируемые электронные или бумажные документы в соответствии с правилами 16 (b) и 26. Если какая-либо из сторон не реализовала и не обдумала политики и методики сохранения информации перед подачей иска в суд, эта сторона может оказаться в невыгодном положении, поскольку ей придется принять участие в обязательном совещании "для достижения согласия" с противными сторонами, которые продумали все заранее и знают, какие предложения обеспечат им наибольшую выгоду.

Кроме того, скорректированные правила явно оговаривают роль электронных данных в процессе заполнения сторонами письменных вопросников (опросных листов) или при физическом формировании документов. Например, правило FRCP 33 (d) позволяет отвечающей стороне указать, что необходимая информация содержится в "бизнес-записях, включая данные, которые хранятся в электронном виде", если (i) ответы могут быть получены из этих записей, (ii) усилия обеих сторон по доступу к этой информации практически одинаковы и (iii) в ответе определены конкретные записи. В соответствии со скорректированным правилом FRCP 34 сторонам явно разрешается указывать желаемое представление электронной информации (распечатанные копии на бумаге или данные в электронном виде), хотя при отсутствии согласия между сторонами или прямого распоряжения суда скорректированные правила подразумевают, что данные, которые хранятсяв электронном виде, будут воспроизводиться в форме, в которой они "обычно обрабатываются" или в другой форме, которую можно считать удобной при разумных предпосылках.

Можно предположить, что формат представления электронных данных станет темой для дискуссий на много лет вперед. Некоторые специалисты уже отметили, что упоминание "формата, в котором данные обычно обрабатываются" потребует представления "файла исходного формата". Другие специалисты возражают, что использование "исходного формата" не позволит легко удалить конфиденциальную информацию или информацию, не подлежащую оглашению, а также не позволит контролировать количество сформированных документов. Некоторые суды и стороны, участвовавшие в процессах, заняли позицию, в соответствии с которой необходимо обеспечить представление документов со всеми их метаданными. Дело *Williams против Sprint/United Management Company,* 230 FRD 640 (D. Kan. 2005); *дело D.E. Tech против Dell Inc.,* 2006 U.S. Dist. LEXIS 87902 (W.D. Va. 2006); дело *Nova Measuring Instruments против Nanometrics Inc.,* 2006 U.S. Dist. LEXIS 49156 (N.D. Cal. 2006); дело *Re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation,* 2007 U.S. Dist. LEXIS 2650 (E.D. N.Y. 2007). Однако в последнее время растет доля судов и специалистов, полагающих, что воспроизведение метаданных не является обязательным. Дело *Kentucky Speedway против National Association of Stock Car Auto Racing Inc.,* 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 2006); дело *Wyeth против Impax Laboratories Inc.,* 2006 U.S. Dist. LEXIS 79761 (D. Del. 2006); *дело The Ponka Tribe of Indians of Oklahoma против Continental Carbon Co.,* 2006 U.S. Dist. LEXIS 74225 (W.D. Okla. 2006). На практике Американская банковская ассоциация опубликовала в 2006 году формальное заключение 06-442,

Можно предположить, что формат представления электронных данных станет темой для дискуссий на много лет вперед.

в котором на юристов возлагается обязанность обеспечить удаление конфиденциальных метаданных либо предоставить суду версию документа без метаданных, чтобы предотвратить возможность воспроизведения по неосторожности метаданных, не подлежащих оглашению. Адвокатуры штатов Флорида и Мериленд возложили схожие обязанности по удалению защищенных метаданных из документа на юридических советников. Пока суды и адвокатуры штатов ведут дебаты об обработке метаданных, следующее утверждение не вызывает сомнений: компании и их юристы должны знать, как хранится их электронная информация и какие метаданные используются при представлении документа. При этом сбор такой информации и подготовка к обсуждению подобных вопросов должны выполняться задолго до совещания с целью "встречи и достижения согласия", назначенного федеральным судом.

В скорректированном правиле 37 также приводится ограниченный список причин, позволяющих избежать санкций за непредоставление электронных данных, если такие данные были утрачены в ходе нормальной работы электронной информационной системы, а принципы работы системы представляются разумными. Как указано выше, суд может не оценить работу системы как разумную, если сторона, участвующая в судебном процессе, не смогла своевременно начать "сохранение данных в связи с юридическим разбирательством". Вопросы получения информации не ограничиваются мейнфреймом; необходимо учитывать носители с резервными копиями, жесткие диски компьютеров,

ноутбуки и другие хранилища электронной информации. Эти вопросы могут оказаться не настолько очевидными, насколько они кажутся с первого взгляда. Используются ли в вашей компании смартфоны, например, компании BlackBerry? Хранятся ли сообщения электронной почты на этих устройствах, а не на серверах компании? Распечатывают ли сотрудники документы (даже если электронные копии регулярно уничтожаются), известно ли, где хранятся распечатанные копии документов? Пользуются ли сотрудники электронными досками объявлений, программами для мгновенного обмена сообщениями или личными адресами электронной почты на работе, и может ли информация об этих действиях попасть в систему управления электронными данными компании? Отслеживает ли компания график удаления или перезаписи электронных данных, можно ли предотвратить удаление или перезапись для определенных данных на основании ключевых признаков (например, имя и фамилия потенциального истца, его должность или продукт, который был приобретен)? Приняты ли в компании четкие политики, регламентирующие сохранение сообщений электронной почты в личных папках сотрудников на компьютерах компании, следуют ли сотрудники этим политикам? Известно ли компании, какие метаданные хранятся на служебных компьютерах сотрудников?

Эффективная система управления электронными данными должна предоставлять ответы на все эти вопросы задолго до возникновения юридического разбирательства, чтобы при возникновении "ситуации юридического разбирательства" компания могла

Эффективная система управления электронными данными должна предоставлять ответы на все эти вопросы задолго до возникновения юридического разбирательства, чтобы при возникновении "ситуации юридического разбирательства" компания могла незамедлительно обнаружить все нужные данные и обеспечить их сохранение в том формате, в котором требуется.

незамедлительно обнаружить все нужные данные и обеспечить их сохранение в том формате, в котором требуется.[32] Под электронными данными, на которые распространяется требование "хранения в связи с юридическим разбирательством" понимаются не только документы, созданные лицом, с которым будет связано возможное юридическое разбирательство, но и любые документы, связанные с этим лицом, а также, в случае возможных заявлений о дискриминации или групповых исков, связанные с другими людьми, находящимися в сходных обстоятельствах.

[32] Allen Smith, *Amended Federal Rules Define Duty to Preserve Work E-mails,* HR NEWS, December 1, 2006.

Благоприятная рабочая среда

В США[33] широко распространена точка зрения, что надлежащие средства фильтрации и мониторинга действий сотрудников являются оптимальными решениями для предотвращения исков о создании неблагоприятной рабочей среды. "Предположение, что использование фильтров необходимо для избежания ответственности, становится все более расхожим".[34] "Многие из исков, связанных с отправкой сообщений электронной почты с сексуальными домогательствами, могли бы быть предотвращены, если бы отправка соответствующего сообщения была бы заблокирована".[35]

Многие из исков, связанных с отправкой сообщений электронной почты с сексуальными домогательствами, могли бы быть предотвращены, если бы отправка соответствующего сообщения была бы заблокирована.

Статистические исследования и беглый анализ исков о создании неблагоприятной рабочей среды показывают, что системы передачи сообщений электронной почты стали причиной бесчисленного множества исков, связанных с вопросами дискриминации и сексуальными домогательствами. Дело *EEOC против Freddie Mac,* Civ. No. 97-1157-A, at 3-4 (E.D. Va. July 24, 1997) (иск подан, рассмотрение иска отложено не менее чем на три года. Причиной иска послужили циркулирующие в компаниисообщения электронной почты со словом "ebonics" (специфический акцент английского языка), унижающие человеческое достоинство. Работодатель был обязан "оперативно принять эффективные меры для пресечения правонарушения". Дело *Olivant против Dept. of Environmental Protection,* 1999 WL 430770 (N.J. Admin. Apr. 12) (распространение сексистского "юмора"

[33] В других странах возможности мониторинга могут быть ограничены или запрещены. Это издание ориентировано в первую очередь на США, хотя, как указано в разделе VIII, для обеспечения соответствия требованиям различных юрисдикций, отличных от юрисдикций США, требуется еще более сложная система управления данными.

[34] Eugene Volokh, Professor of Law UCLA, *Freedom of Speech, Cyberspace: Harassment Law and the Clinton Administration,* 63 LAW & CONTEMP. PROBS. 299 (2000).

[35] Wendy R. Leibowitz, *Avoiding E-mail Horror Stories: Policies and Filters the Best Defense,* N.Y. L.J., December 15, 1998, at 5.

с использованием систем передачи электронной почты представляет собой сексуальное домогательство.); *дело Trout против City of Akron* (Жалоба № CV-97-115879 (подана 17 ноября 1997 г.); вердикт вынесен *id.* (15 декабря 1998 г.)); Город был вынужден выплатить штраф в 260 000 долларов США за то, что коллеги истца просматривали порнографические материалы на своих служебных компьютерах. Напротив, в деле *Delfino против Agilent,* 145 Cal. App.4th 790 (6th Dist., 2006), суд пришел к заключению, что компания не должна нести ответственность за действия своего сотрудника – использование служебного компьютера для рассылки угрожающих сообщений по Интернету, поскольку компания оперативно предприняла необходимые меры, как только получила уведомление о ненадлежащем поведении сотрудника. Кроме того, федеральный закон классифицирует детскую порнографию как "контрабанду," что означает, что обработка, владение, распространение и т. п. таких материалов является незаконным в соответствии со статьей 18 USC 2251 и другими. Действительно, в соответствии с действующим законодательством компания обязана сообщить о любом факте пользования такими материалами в ФБР, в противном случае компания может быть признана виновной в нарушении законодательства о борьбе с детской порнографией.

Чтобы обеспечить защиту от ненадлежащего поведения сотрудников, все больше компаний в США начинают использовать сканирующие устройства или фильтры. Неспособность работодателя в США контролировать передачу электронныхданных, входящих в его систему

и исходящих из нее, может привести к серьезному ущербу. Соответственно, работодатели в США должны информировать сотрудников, работающих в США, что компьютеры являются собственностью работодателя, что они предназначены для выполнения служебных обязанностей, что передача данных может контролироваться в любой момент времени, и что понятие "частной жизни" сотрудника не распространяется на работу со служебным персональным компьютером.[36]

Более того, суды постепенно признают фильтрацию, как наименее ограничивающую меру для защиты сотрудников от оскорбительного содержания, которое может поступить из Интернета. Например, 22 марта 2007 года окружной суд Пенсильвании отклонил акт о защите детей в Интернете [37] как частично противоречащий конституции США, поскольку фильтры были менее ограничивающими средствами защиты детей от доступа к материалам ненадлежащего характера в Интернете, чем те средства, которые упоминались в законодательном акте конгресса США.[38] Суд установил, что фильтры "как правило блокируют примерно 95% материалов ярко выраженного сексуального характера".[39] Также они являются "полностью настраиваемыми, могут настраиваться на различный возраст, а также на разные стили речи либо могут быть полностью отключены…"[40]

С развитием нормативной базы, увеличением количества юридических исков и увеличением стоимости ошибки, которой можно избежать, компании применяют политики использования

С развитием нормативной базы, увеличением количества исков и увеличением стоимости ошибки, которой можно избежать, компании используют политики рабочих мест в дополнение к технологическим мерам, чтобы обеспечить управление продуктивностью, защитить ресурсы и мотивировать сотрудников соблюдать требования нормативных документов.

[36] *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy,* 2001 DUKE L. & TECH. REV. 0026 (2001).
[37] 47 U.S.C. § 231.
[38] *ACLU v. Gonzales,* No. 98-5591 (E.D. Pa. March 22, 2007).
[39] *Id.*
[40] *Id.*

рабочих мест в дополнение к технологическим мерам, чтобы обеспечить управление продуктивностью, защитить ресурсы и мотивировать сотрудников соблюдать требования нормативных документов. По имеющимся данным 80% компаний США или более информируют своих сотрудников, что они могут контролировать изображение на экране компьютера сотрудника, нажимаемые им клавиши и время, проведенное за клавиатурой; 76% контролируют деятельность сотрудников в Интернете; 65% блокируют возможность подключения к веб-сайтам ненадлежащего содержания; 82% открыто заявляют, что компания сохраняет и анализирует файлы, хранящиеся на компьютере сотрудника; 86% уведомляют сотрудников о контроле за сообщениями электронной почты, а 89% уведомляют сотрудников об отслеживании их действий в Интернете.[41] В 2005 году 84% компаний в США приняли политики, регламентирующие использование персональных ящиков электронной почты, 81% располагали политиками использования Интернета, 42% располагали политиками использования программ для мгновенного обмена сообщениями в личных целях, 34% регламентировали работу с личными веб-сайтами в рабочее время, 23% располагали политиками создания личных записей в корпоративных блогах, а 20% корпоративных политик компаний запрещали использование личных блогов в рабочее время.[42] В том же году 26% работодателей признали, что они увольняли сотрудников за нарушение правил использования Интернета, а 25% работодателей увольняли сотрудников за нарушение правил работы с электронной почтой.[43]

[41] AMA/ePolicy Institute Research, *2005 Electronic Monitoring & Surveillance Survey,* (2005).
[42] *Id.*
[43] *Id.*

Защита интеллектуальной собственности является основой успешной работы предприятия

Объем электронной почты увеличивается на 30% в год и составляет примерно 80% интеллектуальной собственности компании.[44] Потенциальные проблемы больше не являются академическими теориями. В деле *Sonoco Products против Johnson,* 23 P.3d 1287 (Co. App. 2001), компания получила почти 7 млн долларов США за неправомерное присвоение коммерческой тайны, когда бывший сотрудник компании и его новый работодатель вошли в сговор с целью совместного использования электронных и физических копий конфиденциальных данных компании Sonoco, украденных сотрудником.[45]

Объем электронной почты увеличивается на 30% в год и составляет примерно 80% интеллектуальной собственности компании.

Суды не только признали виновным сотрудника, укравшего электронные данные, но также привлекли к ответственности нового работодателя. В деле *Shurgard Storage против Safeguard Self-Storage,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000), истец подал иск против следующего работодателя своего бывшего сотрудника в соответствии с законом о компьютерных преступлениях, поскольку бывший сотрудник истца использовал служебные компьютеры для пересылки конфиденциальной информации истца по электронной почте в компанию-ответчик, а затем компания-ответчик приняла бывшего сотрудника истца на работу. В деле *Charles Schwab против Carter,* 2005 U.S. LEXIS 21348, no. 04-C-7071 (N.D. Ill. Sept. 27, 2005), суд постановил, что истец успешно обосновал причины для проведения судопроизводства против нового работодателя

[44] Frank Chambers, *EDD Tips for Email from the Front Line,* LAW TECHNOLOGY TODAY, March 2007.
[45] *См. также дело Sawyer против Dept. of Air Force,* MSPB 1986, 31 MSPR 193; *дело US против Middleton,* 35 F. Supp. 2d 1189 (N.D. Cal. 1999); *дело EF Cultural Travel BV против Explorica Inc.,* 274 F.3d 577 (1st Cir. 2001); *дело Pacific Aerospace Electronics Inv. против Taylor",* 295 F. Supp. 2d 1188 (E.D. Wa. 2003).

бывшего сотрудника компании в соответствии с законом о компьютерных преступлениях, исходя из предпосылки об опосредованной ответственности. Пока сотрудник работал в компании-истце Schwab, он отправлял конфиденциальную информацию компании Schwab по электронной почте в компанию Acorn, куда затем перешел на работу. Компания Schwab утверждала, что компания Acorn побуждала сотрудника осуществлять доступк компьютерным системам компании Schwab, выходящий за рамки должностных обязанностей работника.

В деле *Lowry's Reports против Legg Mason,* 271 F. Supp. 2d 737 (D. Md. 2003), сотрудник распространял и воспроизводил материалы, охраняемые авторским правом, на рабочем месте. Суд отметил, что тот факт, что работодатель не знал о поведении сотрудника (после того как работодатель потребовал от работника прекратить распространение материалов, охраняемых авторским правом), не относится к делу. Присяжные вынесли вердикт на сумму в 20 млн долларов США.[46]

Решения по перечисленным делам наглядно демонстрируют, что если бы американская компания, признанная виновной, контролировала потоки возможного распространения конфиденциальной информации и была бы способна заблокировать или отфильтровать несанкционированную отправку такой информации, то такая компания смогла бы не только избежать многолетних судебных разбирательств, но и предотвратить раскрытие своей конфиденциальной информации. В конце концов, независимо от решения суда по конкретному иску попытки "поместить зубную пасту обратно в тюбик" редко бывают удачными.

[46] Попытки подачи нового иска и открытия судопроизводства были отклонены в ходе рассмотрения дела *Lowry's Reports, Inc. против Legg Mason, Inc.,* 302 F. Supp. 2d 455, 461 (D. Md. 2004).

Конфиденциальность. Когда СМИ (слишком много информации) – это плохо[47]

В отличии от стран Европейского Союза (ЕС) и некоторых других регионов мира, в США не существует общепринятой схемы обеспечения конфиденциальности данных. Напротив, законы США стремятся описать вопросы конфиденциальности данных для конкретного сектора рынка или индустрии, при этом принимаются отдельные законы, которые регламентируют создание, хранение, использование и доступ к персональным конфиденциальным данным. В отличии от FRCP, регламентирующего в первую очередь хранение данных, или методик мониторинга, представленных в делах о создании неблагоприятной рабочей среды или о нарушении закона о компьютерных преступлениях, законодательство, связанное с персональными данными, регламентирует и ограничивает набор данных, которые компания имеет право собирать, обрабатывать, передавать, хранить, использовать или распространять. Важно, что эффективные системы управления информацией должны не только позволять сохранять и архивировать данные, когда это необходимо, а также обеспечивать мониторинг при использовании в США, если это возможно. Такие системы должны также обеспечить введение ограничений на использование и доступ к персональной информации, которая была передана компании для определенных четко оговоренных целей.

[47] Подробнее о нормах обеспечения конфиденциальности, принятых не только в США, но и в других странах см. Baker & McKenzie *Справочник по мировым нормам обеспечения конфиденциальности* (International Association of Privacy Professionals) ©2006.

Закон о преемственности страхования и отчетности в области здравоохранения (HIPAA) регламентирует сбор, использование и доступ к медицинским данным для "соответствующих организаций", к которым отнесены организаторы медицинских программ, бухгалтерские подразделения организаторов медицинских программ и учреждения здравоохранения, передающие медицинские данные.

Например, Акт Грэмма-Лича-Блайли устанавливает правила обработки информации в финансовых институтах, включая компании, работающие в банковской сфере, сфере страхования, работающие с акциями и облигациями, предоставляющие финансовые консультации, а также инвестиционные компании. Положения этого документа вводят меры для защиты от продажи конфиденциальной финансовой информации, регламентируют методы, которые позволяют защититься от методов социального инжиниринга, используемых для получения личной финансовой информации путем выдачи себя за другого человека, а также позволяют потребителям отказаться от ограниченного предоставления "необщедоступной личной информации". Кроме того, теперь финансовые институты обязаны реализовывать программы по обеспечению информационной безопасности, которые соответствуют определенным критериям, установленным соответствующим регулирующим органом, например, стандартам Федеральной торговой комиссии США по защите информации потребителей.

Закон о предоставлении достоверных данных о кредитоспособности (и многие схожие с ним законы штатов) в первую очередь регламентирует использование и раскрытие информации в "отчетах о потребителях", которые формируются "агентствами по формированию отчетов о потребителях", чтобы не допускать слишком широкой трактовки понятия "информация". Закон устанавливает ограничения на сбор, использование и раскрытие медицинских данных, финансовой информации и материалов

судебных слушаний, а также регламентирует специальные ограничения, связанные с проблемами кражи личности, отчетами о потребителях для трудоустройства и "аналитическими отчетами о потребителях", которые формируются для сторонних организаций или третьих лиц. В законе содержится множество требований к агентствам, формирующим отчеты о потребителях, а также к получателям отчетов о потребителях по обеспечению целостности и точности собранной и распространяемой информации, а также по доступу к отчетам о потребителях по Интернету, использованию этой информации и ее безопасному уничтожению.

Положения HIPAA распространяются на использование и раскрытие конфиденциальной медицинской информации, представленной в любом формате.

Закон о преемственности страхования и отчетности в области здравоохранения (HIPAA) регламентирует сбор, использование и доступ к медицинским данным для "соответствующих организаций", к которым отнесены организаторы медицинских программ, бухгалтерские подразделения организаторов медицинских программ и учреждения здравоохранения, передающие медицинские данные. Положения HIPAA распространяются на использование и раскрытие конфиденциальной медицинской информации, представленной в любом формате. В вышеупомянутых организациях должна быть введена должность ответственного за обработку данных, который отвечает за внедрение и выполнение политик и методик, установленных HIPAA, а также обязан обеспечить хранение записей в течение шести лет. Кроме того, эти организации должны выполнять требования отдельных стандартов обеспечения безопасности для

защиты конфиденциальных медицинских данных, хранящихся в электронном виде, 45 CFR 160 и 164. В январе 2007 года министерство юстиции США объявило об открытии первого дела по нарушению HIPAA, в ходе которого было выдвинуто обвинение, связанное с кражей медицинских данных, включая 1130 электронных записей из клиники Кливленда. Предполагается, что сотрудник клиники использовал компьютерную систему клиники для сбора и продажи записей пациентов организованной преступной группе, которая использовала записи пациентов для выставлении организатору медицинской программы Medicare фальшивых счетов на сумму 7 млн долларов США. Кроме того, обработка медицинских данных регламентируется различными законами штатов, например, законом штата Калифорния о конфиденциальности медицинских данных.[48]

Во многих штатах также приняты законы, содержащие четко выраженные требования по обеспечению конфиденциальности номеров социального страхования. Например, статья 1798.85 Гражданского кодекса штата Калифорния запрещает, среди прочего, запрашивать у частного лица его (ее) номер социального страхования по Интернету, если соединение не является защищенным или номер социального страхования не зашифрован. Статья 1798.81.5 Гражданского кодекса штата Калифорния требует от компаний реализовать разумные процедуры обеспечения безопасности широкого спектра личных данных, включая номера социального страхования, номера кредитных карт и банковских счетов, номера автомобильных прав и т. п. В штате Нью-Йорк действует сходный закон,

[48] В ходе недавних исследований 98,5% респондентов ответили, что учреждения здравоохранения несут ответственность за обеспечение безопасности медицинских записей пациентов, но менее 40% респондентов выразили уверенность, что их медицинские учреждения обеспечивают надежную защиту их медицинских данных. Практически все респонденты верят, что учреждения здравоохранения юридически обязаны уведомлять пациентов, если кто-то получил доступ к медицинским записям пациента без его согласия, однако 7 из 10 респондентов не уверены, что учреждения здравоохранения соблюдают требования о необходимости уведомления пациентов о возможном нарушении безопасности. www.epictide.com.

регламентирующий процедуры уничтожения документов, содержащих персональные данные, например номера социального страхования.[49]

Компаниям следует тщательно выбирать системы управления электронными данными, чтобы обеспечить выполнение быстро развивающихся требований по обеспечению конфиденциальности данных. Врачу и банкиру требуются средства шифрования, позволяющие защитить конфиденциальную информацию (как медицинскую, так и финансовую) от раскрытия по неосторожности. Чтобы предотвратить несанкционированное или слишком широкое распространение информации, необходимо устанавливать межсетевые экраны и средства контроля и разграничения доступа. Необходимо использовать средства мониторинга, позволяющие предпринять необходимые меры и сделать соответствующие уведомления при обнаружении нарушения безопасности. Нарушения федеральных законов США и законов штата не только часто приводят к уголовной ответственности, но и негативно сказываются на бизнесе компании и ее бренде. Опять же, заблаговременное планирование является более предпочтительным, чем попытки экстренного восстановления ущерба.

Нарушения федеральных законов США и законов штата относительно обеспечения конфиденциальности информации не только часто приводят к уголовной ответственности, но и негативно сказываются на бизнесе компании и ее бренде. Опять же, заблаговременное планирование является более предпочтительным, чем попытки экстренного восстановления ущерба.

[49] NY CLS Gen. Bus. §399-h (2007).





Шифрование

Шифрование является необходимой, хотя пока что зачастую недостаточно распространенной технологией. "Шифрование данных определяется как процесс преобразования передаваемой или хранимой информации, позволяющий предотвратить ее прочтение до выполнения обратного преобразования легитимным получателем."[50] Использование средств шифрования для защиты конфиденциальной информации и информации, являющейся коммерческой тайной, при передаче по Интернету является необходимостью.

Если в организации не используются средства шифрования, компания практически не обеспечивает защиту своих секретов. "Специалистам в сфере информационной безопасности 2005 год запомнился как год, в котором вопросы утечки данных оказались в центре внимания общества. Общественный интерес был во многом вызван принятием новых законов США, обязывающих организации делать публичные уведомления о случаях кражи или утраты данных своих клиентов".[51] Более серьезным фактором, вызывающим беспокойство, стало то, что сотрудники, которым предоставлен доступ к конфиденциальным данным работодателя, либо не уделяют должного внимания вопросам защиты информации, либо не умеют пользоваться средствами защиты информации. В рамках статьи для семинара "Почему Джонни не может зашифровать данные"[52] два исследователя из университета Карнеги-Меллон

[50] Fred Moore, *Preparing for Encryption: New Threats, Legal Requirements Boost Need for Encrypted Data,* COMPUTER TECHNOLOGY REVIEW, August-September 2005.
[51] Kevin Murphy, *Email Security Uncovered,* COMPUTER BUSINESS REVIEW ONLINE, November 1, 2005 (quoting Alex Hernandez, director of advanced product development at CipherTrust).
[52] Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0,* доступно на странице http://www.gaudior.net/alma/johnny.pdf.

обнаружили, что типовой пользователь, обладающий достаточным уровнем квалификации и навыками работы с системой электронной почты, не умеет пользоваться средствами шифрования. Последующее исследование "Почему Джонни по-прежнему не может зашифровать данные"[53] показало, что ситуация практически не изменилась. Компании должны активно внедрять удобные для пользователей системы шифрования, которые соответствуют потребностям компании, а затем проводить обучение пользователей работе с новыми системами.

Использование систем хранения данных, в которых находится незашифрованная информация, служит для компании причиной риска кражи информации о клиентах, что может привести к негативным отзывам в средствах массовой информации, потере клиентов и дорогостоящим судебным разбирательствам. Например, в январе 2007 г. группа компаний TJX, в которую входят сети розничной продажи T.J. Maxx, Marshalls, Home Goods, Bob's Stores и другие, объявила о фактах несанкционированного доступа в ее компьютерные системы в течение 2005 – 2006 гг. Действия злоумышленников привели к краже информации о 45,7 миллиона платежных карт клиентов, которые использовались для оплаты покупок с 2002 по 2004 год. Злоумышленники получили номера кредитных и дебетовых карт, а также имена держателей карт.[54] В марте 2007 года сеть магазинов Radioshack обнаружила, что в 20 ящиков документов, подлежащих утилизации, попали чеки с номерами кредитных карт потребителей.

[53] Steve Sheng et al, *Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software,* доступно на странице http://cups.cs.cmu.edu/soups/2006/posters/sheng-poster_abstract.pdf.
[54] TJX, Часто задаваемые вопросы (на англ. языке), www.tjx.com/tjx_faq.htm.

Генеральный прокурор штата Техас инициировал соответствующее расследование. В марте 2007 года сотрудники компании Group Heath Cooperative Healthcare System потеряли два ноутбука, в которых хранились имена, адреса, номера социального страхования местных пациентов и сотрудников, а также их идентификаторы в рамках программы.

Ущерб от любого из этих инцидентов можно существенно снизить путем использования шифрования. Особенно уязвимыми оказываются средние компании. Злоумышленники больше не ищут славы создателя вируса, распространившегося по всему миру. Вместо этого злоумышленников интересуют деньги. Поскольку злоумышленникам известно, что затраты средних компаний на системы защиты и средства шифрования, как правило, не особенно высоки, предполагается, что более 4000 средних компаний могут оказаться особенно уязвимыми для атак, если они не внедрят соответствующие средства защиты информации.[55]

Как указывалось выше, использование средств шифрования является обязательной мерой для защиты от случайного раскрытия персональных данных, по крайней мере, оно является обязательным в соответствии с законом об обеспечении конфиденциальности номеров социального страхования штата Калифорния.[56] Кроме того, использование различных стандартов шифрования является обязательным для использования всех подрядчиков по правительственным контрактам США, связанным

Поскольку злоумышленникам известно, что затраты средних компаний на системы защиты и средства шифрования, как правило, не особенно высоки, предполагается, что более 4000 средних компаний могут оказаться особенно уязвимыми для атак, если они не запланирует внедрение соответствующих средств защиты информации.

[55] Allan Holmes, *Many Mid-Market Enterprises Say They Have Neither the Time, Money nor Resources to Spend on Security. Which May Be Why the Crooks Are Targeting Them and Turning the Mid-Market into a Bad Neighborhood,* CIO, March 1, 2007.
[56] CAL. CIV. CODE §1798.29 (part of bill also known as SB 1386).
[57] National Institute of Standards and Technology (NIST), Data Encryption Standard Fact Sheet, доступно на странице http://csrc.nist.gov/cryptval/des/des.txt.

с созданием вычислительных систем.[57] Наконец, шифрование конфиденциальной информации для предотвращения ее непреднамеренного раскрытия является просто разумным. ИТ-подразделение и юридическое подразделение должны совместно определить потребности компании в средствах шифрования и установить, обеспечивает ли существующая система надежную защиту от взлома, кражи информации или судебного разбирательства.

[57] National Institute of Standards and Technology (NIST), Data Encryption Standard Fact Sheet, доступно на странице http://csrc.nist.gov/cryptval/des/des.txt.

Международное законодательство. Противоречия в нормативных требованиях к обработке данных

Требования к сбору данных, их обработке, хранению, использованию, мониторингу, доступу и уничтожению данных в различных юрисдикциях за пределами США не только отличаются от американских, но в некоторых случаях впрямую противоречат законам США. Компаниям, которые осуществляют свою деятельность в различных странах мира, необходимо выполнять требования местных нормативных документов, регламентирующих обработку данных, а также правила передачи электронной информации через границы государств.

Компаниям, которые осуществляют свою деятельность в различных странах мира, необходимо соблюдать требования местных нормативных документов, регламентирующих обработку данных, а также правила передачи электронной информации через границы государств.

Например, каждая из стран Европейского Союза, в соответствии с директивой ЕС об обеспечении конфиденциальности информации, внедряет законодательство, регламентирующее сбор, запись, организацию, хранение, адаптацию, изменения, считывание, блокирование, мониторинг, использование, раскрытие, передачу, перемещение и уничтожение "информации, являющейся персональной", и в некоторых случаях требующее использования более развитых систем защиты для "конфиденциальной информации, являющейся персональной". В отличии от США, в странах ЕС понятие "информации, являющейся персональной" определено достаточно широко и, как правило, не ограничивается индустрией или сектором рынка. Вместо этого законодательные акты запрещают

несанкционированную обработку или передачу персональных данных, включая имя и фамилию, адрес, сведения о заработной плате, доходе и другую финансовую информацию, а также аналогичные действия с "конфиденциальными" персональными данными, включая сведения о здоровье, расовой или этнической принадлежности, политических взглядах, участии в работе общественных организаций или семейном положении. Действие этих законов распространяется не только на сотрудников, но и на клиентов компаний. Италия, Австрия и несколько других стран сделали дальнейшие шаги и распространили принципы обеспечения конфиденциальности данных не только на частных лиц, но и на компании.

Поскольку Европейский Союз рассматривает США как "небезопасную юрисдикцию", такая информация не может быть законно передана в электронном или любом другом виде в США или в другие "небезопасные юрисдикции", если только не приняты определенные меры предосторожности, например участие в соглашении между США и ЕС по вопросам защиты персональных данных, принятие моделей оговорок ЕС или реализация утвержденных ЕС политик обеспечения конфиденциальности данных. Даже если внедрение соответствующих мер защиты обеспечивает возможность передачи персональных данных в США, этого может оказаться недостаточно для получения разрешения на "дальнейшую передачу" персональных данных неустановленным сторонним компаниям, выполняющим обработку данных, или передачу в другие страны, например

службам ввода данных в Индию. И речь не только о странах ЕС: Канада, Аргентина, Япония, Австралия и многие другие страны также требуют использования различных средств обеспечения конфиденциальности информации.

Компании вынуждены не только определять, какие данные можно собирать, обрабатывать и передавать заграницу, им также необходимо балансировать, соблюдая взаимодополняющие, а иногда и противоречащие друг другу законы. Например, в соответствии с SOX компании, акции которых представлены на бирже, должны поддерживать горячую линию, по которой они принимают анонимные сообщения о возможных нарушениях в сфере финансовых операций и операций с ценными бумагами. Идея, реализованная в положении SOX о горячей линии для анонимных сообщений, заключалась в создании для сотрудников комфортной ситуации, в которой они могут остаться неизвестными и не бояться ответных мер. Напротив, страны ЕС не приветствуют создание горячих линий для анонимных сообщений, считая это нарушением прав на частную жизнь, и ограничивают возможности для передачи анонимных сообщений. Конфликт положений SOX о "прозрачности" и ЕС о защите частной жизни создает очевидную дилемму для транснациональных компаний, акции которых представлены на бирже, и требует создания сложных систем управления данными, обеспечивающих необходимые функции хранения информации в течение надлежащего интервала времени, доступа и получения этой информации, а также соответствующих требованиям SOX.[58]

Компании вынуждены не только определять, какие данные можно собирать, обрабатывать и передавать за границу; им также необходимо балансировать, соблюдая взаимодополняющие, а иногда и противоречащие друг другу законы.

[58] Подробнее о вопросах глобализации кодексов поведения и международном опыте использования горячих линий для анонимных сообщений читайте в статье Синтии Л. Джексон *"Излишняя глобализация кодекса поведения может привести к нарушению закона" ("Overreaching Global Codes of Conduct Can Violate the Law")*, опубликованной в журнале "LA and SF Daily Journal" 7 июня 2006 г.

Другие "рекомендованные методики", принятые в США, просто невозможно реализовать за границей. Например, в 2001 году Верховный суд Франции постановил, что увольнение французской компанией своего сотрудника – гражданина Франции, о котором в результате мониторинга его служебного компьютера стало известно, что он отправляет потенциальному конкуренту по электронной почте конфиденциальную информацию компании не только было неправомерным, но противоречило Конституции Франции и являлось уголовным преступлением. Французский суд подтвердил, что сотрудник обладает конституционным правом на частную жизнь в течение своего рабочего времени и на своем рабочем месте несмотря на то, что работодатель запретил использование служебного компьютера в нерабочих целях. Германия занимает несколько более мягкую позицию в этом вопросе, но также ограничивает возможности мониторинга служебных компьютеров сотрудников, если работодатель разрешает сотрудникам использовать корпоративные системы в личных целях.
В некоторых юрисдикциях ЕС для выполнения мониторинга действий сотрудников требуется, как минимум, регистрация и утверждение мониторинга в местном органе, отвечающем за соблюдение законодательства о защите частной жизни.

Таким образом, при выборе системы управления электронными данными компания должна осознавать юридические требования той страны, в которой выполняется сбор, использование или доступ к данным. Если, как в случае транснациональных компаний, данные создаются или передаются

в различных юрисдикциях, необходимо соблюдать местные законы об обеспечении конфиденциальности данных, а также реализовать соответствующие правила контроля и разграничения доступа и правила фильтрации на межсетевых экранах во всех системах обработки данных, чтобы предотвратить возможность обработки, мониторинга или передачи данных без соблюдения надлежащих мер защиты, соответствующих требованиям законодательства.





Полезный практические рекомендации

1. **Планируйте заранее.** Не ждите судебного процесса, жалобы на создание неблагоприятной рабочей среды, утечки информации, составляющей коммерческую тайну, или раскрытия конфиденциальной информации, чтобы начать активное управление данными компании.

2. **Изучайте требования законодательства.** Проанализируйте требования законодательства индустрии и юрисдикций, в которых работает ваша компания. Например, какие требования по хранению данных предъявляются к конкретной информации в стране или в штате? Какие средства защиты используются для контроля и разграничения доступа, а также для хранения данных? Известно ли, какую информацию необходимо шифровать и какие существуют обязательства по уведомлениям в случае нарушения безопасности? Допускается ли в этой юрисдикции использование фильтров для предотвращения создания неблагоприятной рабочей среды, или использование фильтров считается вторжением в частную жизнь?

3. **Универсального решения не существует.** Если ваша компания работает на внутреннем или на международном рынке, изучите порой противоречивые требования, которым должна соответствовать система управления электронными данными. Рассмотрите возможность внедрения межсетевых экранов, механизмов контроля и разграничения доступа, а также отключения определенных функций в юрисдикциях, в которых не допускается мониторинг служебных компьютеров или использование средств фильтрации.

4. **Распределите ответственность за управление системой.** Назначьте сотрудников, ответственных за обслуживание и управление электронными данными. Это может быть совместная группа сотрудников ИТ-подразделения и юридического подразделения, в работе которой принимают участие сотрудники отдела кадров и других подразделений. Как можно раньше привлекайте к работе сотрудников, которым потребуется обеспечить работоспособность системы при возникновении юридической необходимости.

5. **Определите различные форматы и местоположения хранения данных.** Помните, что данные могут храниться в столах, КПК , домашних компьютерах, ноутбуках и т. д. Перед тем как обеспечить управление данными, за которые компания считается ответственной по закону, необходимо определить комплекс мер, которые позволят убедиться в том, что внедряемая система позволяет собирать необходимую информацию. Проанализируйте существующие метаданные.

6. **Выбирайте гибкую систему управления электронными данными.** Выбирайте систему, которая обладает достаточной гибкостью, чтобы соответствовать нуждам вашей компании по вопросам хранения, архивирования, мониторинга, фильтрации и шифрования в юрисдикциях, в которых компания ведет свою деятельность. Выбирайте систему, которая удобна для пользователей, чтобы сотрудники не тратили лишнее время на ее освоение. Выбирайте систему, которая сможет адаптироваться к изменяющимся требованиям законодательства. Выполняйте планирование с учетом увеличения и усложнения структуры данных, включая метаданные.

7. **Не заражайтесь болезнью накопления.** То, что технология позволяет вашей компании хранить

большие объемы данных, не означает, что это обязательно нужно делать. Необоснованное хранение лишних данных не только затрудняет получение нужных данных, но и повышает риск раскрытия информации. Например, не храните конфиденциальные финансовые данные клиентов, если они не требуются для вашей работы. Если информацию такого рода необходимо хранить, обязательно зашифруйте ее.

8. **Используйте политики.** Разрабатывайте и внедряйте четкие и простые политики, соответствующие положениям действующего законодательства, касательно хранения документов, учитывая необходимость "хранения документов в связи с судебным разбирательством" задолго до начала судебного разбирательства. В США используйте зарекомендовавшие себя политики мониторинга электронной почты сотрудников. Используйте политики шифрования конфиденциальной информации для предотвращения раскрытия такой информации по неосторожности. Если это возможно, реализуйте механизм дисциплинарных санкций, чтобы продемонстрировать сотрудникам, что политики обязательны к соблюдению.

9. **Будьте готовы.** Не затягивайте разработку процесса сохранения данных в связи с юридическим разбирательством до тех пор, пока не возникнет "ситуация юридического разбирательства" (не говоря о судебном иске). Предусмотрите процесс, позволяющий предотвратить удаление документов, чтобы при необходимости быстро перевести систему в режим "сохранения данных в связи с юридическим разбирательством". Готовьтесь к любому слушанию в суде по вопросам "встречи и достижения согласия", связанным с использованием технологии e-Discovery.

Участники юридического разбирательства, которые знают, чем они располагают и почему они этим располагают, получат преимущество при планировании использования технологии e-Discovery. Не дожидайтесь нарушения безопасности, чтобы внедрить процессы оперативного уведомления и формирования отчетов.

10. **Обучайте и контролируйте, затем снова обучайте и снова контролируйте.** Политики и система управления данными работают только в том случае, если сотрудники знают, как пользоваться предоставленными им средствами. Для достижения нужного результата требуются скрупулезное согласованное внедрение и тщательное техническое обслуживание системы. Приобретение системы управления данными – лишь первый шаг на пути к обеспечению соблюдения требования нормативных документов. Появление новых данных, новых технологий, новых законов, новых угроз и новых сотрудников потребуют тщательной настройки системы и проведения постоянного обучения и контроля.













WP33-0705

postini